September 25, 2008

Drug Enforcement Administration
Attention: DEA Federal Register Representative/ODL
8701 Morrissette Drive
Springfield, VA 22152

Re: Docket No. DEA-218, Electronic Prescriptions for Controlled Substances

Dear Sir or Madam,

Epic is one of the leading developers of Electronic Health Records systems in the country. Our customers collectively care for more than one fifth of the population of the United States. All of our customers' clinical systems incorporate e-prescribing capabilities and we appreciate this opportunity to comment on the proposed regulations. While we and our customers are in favor of new regulations that would make it possible and safe to electronically prescribe controlled medications, thereby furthering our goals of patient safety through electronic prescriptions and medication reconciliation, we have a number of concerns with the regulations as proposed.

As written, the proposed regulations will result in significant overhead and additional time both on a per-prescription and total-practice basis that is not in line with the risk reduction they are intended to provide. As a result, practitioners and many organizations may choose to use only paper prescriptions as they offer a less rigid, easier to meet, and more cost-effective option. Adoption of e-prescribing is being pushed by public policy, and thus we encourage the DEA to provide rules that facilitate adoption rather than stifle growth. Otherwise, many practitioners, pharmacies, and patients will likely miss out on the benefits of e-prescribing.

Our specific comments are organized by Code of Federal Regulation part.

§ 1300.03 Definitions relating to electronic orders for controlled substances and electronic prescriptions for controlled substances.

Definition of "Service Provider"

The term service provider is used throughout the proposed regulation in a way to imply a single entity being the service provider. For many organizations, multiple groups may provide the distinct services. Common examples of groups that may provide one or more of these services include a healthcare organization's IT staff, an EMR system vendor, and consulting firms.

We request that the regulations be more specific to the types of services being provided. For example, documenting in-person identity proofing and enabling the proper prescription writing security in the system would be a function of the group administering system configuration. A system vendor would need to supply software with the appropriate security levels that enable the administration group to limit prescription writing to authorized providers.

§ 1311.105 In-person identity proofing

What are the requirements when the entity documenting the in-person identity proofing is the same entity that is conducting the in-person identity proofing? As in the case where a hospital/clinic's staff will

be the one's conducting the in-person identity proofing and the hospital/clinic's IT staff will be documenting having that in-person identity proofing.

§ 1311.110 Two-factor Level 4 authentication

The Certification Commission for Healthcare Information Technology (CCHIT), which is the sole certification body authorized by the Department of Health and Human Services to certify EHRs and e-prescribing functionality, has not yet required certified systems to require two-factor authentication. Based on the 2007 security requirements line number S31 this requirement is on the roadmap for May 2009 and beyond. Based on the 2008 requirements, criteria number SC 03.13, this requirement is on the roadmap for 2010 and beyond. The requirement as currently stated by CCHIT is to support NIST 800-63 level 3 authentication.

CCHIT 2007 Ambulatory Security Final Criteria:
http://www.cchit.org/files/Ambulatory_Domain/CCHIT_Ambulatory_SECURITY_Criteria_2007_Final__16Mar07.pdf

CCHIT 2008 Ambulatory Final Criteria:
http://www.cchit.org/files/certification/08/Ambulatory/CCHITCriteriaAMBULATORY08FINAL.pdf

As a result, this may impose greater challenges and changes than documented.

The requirement that the system require two factor level 4 authentications should be changed as a result to reflect the current security requirements imposed by the CCHIT. Future changes to regulations to then require two-factor level 4 authentications should take into account the time required to upgrade to the version of the software that meets the latest CCHIT requirements.

The use of two-factor level 4 authentication will also impose additional financial burden onto practitioners and healthcare organizations. When combined with the added workflow complexity of using two factor level 4 authentication, many practitioners and healthcare organizations will choose to continue to use paper prescriptions.

§ 1311.110 Automatic lockout after a period of inactivity

In a full fledge EHR where the system is often in the exam room where the practitioner is performing tasks other than e-prescribing, a two-minute timeout setting is not realistic as it can take more than two minutes to perform an exam.

Instead of requiring an automatic lockout after two minutes, we recommend that authentication be the act of signing and thus authentication and the finalization of signing occur together. This will prevent any potential diversion from occurring.

§ 1311.115 Prescription must contain all DEA data elements

How would a homeless person's address be represented in such a way that a pharmacist knows the patient has no address versus a required field being missing?

§ 1311.120 Present the required data elements to the practitioner

The patient's address (demographics) information is a registration and check-in process to put the patient on the provider's schedule of patients. The provider uses the patient's name and date of birth to select the correct patient. Patient address is not used currently by physicians as a method for patient identification or selection.

§ 1311.120 Indicate that each prescription is ready to be signed

This adversely impacts the workflow of the prescriber as it will require additional steps. Currently, many systems clearly show in a separate area of the application what will be signed. An alternative suggestion is a clear marking of controlled medications such that it would be clear if controlled medications will be signed.

§ 1311.125 Authenticate to the system just before signing

As listed in relation to the two-minute timeout setting, we recommend that the act of authentication be the completing step of signing rather than prior to initiating the signing function, though it should be initiated by a signing function, such as clicking of a Sign button within the application. This would be in addition to initial authentication for access to patient data and system functions.

Currently prescribers already understand that the act of signing means they are responsible for the prescription's accuracy and necessity. Windows for click-through agreements that are on many computer systems are typically unread and passed through without consideration. As such, it seems reasonable to collect the statement once for the practitioner and keep that on file. This would provide the DEA legal documentation that the practitioner understood that the signing function was their legal authorization of the prescription and not put unnecessary additional steps in the signing process.

§ 1311.125 Indicate that the prescription was signed § 1311.125

Including a yes/no indication in the message is possible but in the case where this is not indicated, what is the requirement of the downstream systems in response to a negative indication? Would the requirement be that they error the data file back to the originating system and report the incident to the DEA?

§ 1311.130 Do not transmit if printed; do not print if transmitted

How does the functionality of a patient receipt of medications to be picked up at the pharmacy work with this regulation? A patient receipt is a listing of all medications that were prescribed during the office visit. It would indicate which pharmacies the medications were sent to and the method of transmission (print, fax, call-in, or electronically). The driving need behind such functionality is that patients need to know which medications were prescribed so that they can ask questions of the prescriber during the encounter as well as remember the medications to pick up.

§ 1311.130 First recipient digitally signs the prescription as transmitted

How is the first recipient defined? In the following series of events at what point is the digital signature then required.

1. Provider views and signs order on the GUI front end.
2. Information from the GUI front end is transmitted to the server.
3. On the server the information is stored.

4. The electronic data file contents is generated from that stored information.
5. The electronic data file's contents is sent from server to a web server to then send the data file to the intermediary.
6. Intermediary receives the file. Additional routing through intermediary recipients may also be done during this step.
7. Intermediary sends file to the pharmacy's portal outside of the firewall.
8. Pharmacy portal receives the file and passes through the firewall and onto the pharmacy web server.
9. Web server sends the file or file's contents to server for processing, and the prescription record is created and stored.

Does the first recipient change for a system hosted by a healthcare organization versus an ASP model?

In the case of a direct interface between the prescribing and dispensing systems does the first recipient change when no intermediary is used to transmit?

Clarification of who in the life cycle of an electronic prescription is the first recipient of the prescription is the only way to ensure compliance as well as legal responsibility. We request detailed precedent examples to provide this clarification to ensure baseline for contract and compliance.

§ 1311.135 Revocation of access authorization

What are the technical specifications for this database?

Via what method would a healthcare organization gain access to this database?

Would the data be of a nature that privacy or security measures should be taken?

Without further technical detail about the possibility to automate this process, checking this database weekly may create a burden for healthcare organizations. A large organization may have thousands of practitioners.

The requirement to provide 24/7 support to allow a practitioner to alert of a lost/stolen token so that it can be immediately disabled would be an additional cost to the service provider performing system authentication support. Are automated services to allow the provider to deactivate a token acceptable?

§ 1311.140 Generate monthly logs for practitioner review

The proposed monthly log to review seems to provide a method for providers to spot diversion under their name within the system. It does not provide a solution to cross reference that list against the pharmacy system to allow for full review to ensure no diversion occurred further downstream.

A monthly log may be an effective means to prevent diversion, but that seems unlikely due to the volume of prescriptions to be reviewed.

§ 1311.160 First pharmacy (or last transmitter) digitally signs the prescription as received

In the case of an integrated system where the order is ordered and dispensed from within the same system, is a digital signature required within the pharmacy? To clarify, there are no transmission/interfacing/intermediaries in this scenario.

It is our understanding that there is no human interaction needed at the point the order is digitally signed on receipt within the pharmacy system. That is, the pharmacy application can digitally sign the prescription automatically in the background. Is this correct?

§ 1311.165 Check the validity of the prescriber's DEA registration (Pharmacy)

Can the CSA database be queried via a real-time interface from the HIS, or does it need to be imported on a weekly basis by the HIS?

If the provider is not in the CSA database yet, or the CSA database doesn't contain the provider (for example, there is an error in the most recently imported CSA database), yet after researching (for example, query using a web application with direct access to the CSA database), it's determined the provider is allowed to place orders for controlled substances. What sort of tracking/auditing/authorization is needed to perform this manual CSA validation? Should the system allow some sort of override functionality for the CSA validation?

Similarly, what if the DEA number received with the order is incorrect (for example, transposed numbers). Can the pharmacy system modify the DEA number so that it is correct, or do they need to reject the prescription?

With an integrated ordering and pharmacy system, assuming the organization is validating providers weekly (see point 1311.135), does the pharmacy system need to validate the DEA number of the provider against the CSA database? To clarify, if the ordering system will never allow an unauthorized user to sign a controlled substance, then the pharmacy system will never receive a controlled substance from an unauthorized user.

If the electronic ordering and pharmacy system's are required to query the CSA database, then the CSA database's architecture will need to efficiently support electronic queries for discrete data elements. For example, asking the electronic system to validate that the provider's name from the order matches the provider's name associated with the DEA number could be problematic (for example, Jon D. Doe is not the same as Jon Doe).

When dealing with electronic prescriptions, the more secure methodology would be to prevent prescribers from placing orders if their DEA registration is revoked or suspended rather than trying to catch the order on the backend when it has reached the pharmacy.

§ 1311.170 Have an internal audit trail and analyze for auditable events (Pharmacy)

What can be changed on a controlled substance during processing of the prescription in pharmacy? Can the dose be changed? Can the product be changed (for example, 5 mg changed to 10 mg, and the sig is changed from "take 2 tablets daily" to "take 1 tablet daily")? Can the patient instructions be changed (for example, "take daily" to "take daily before breakfast")?

Are these audit reports limited to information changed at the order level, such as administration instructions, or does it also apply to changes made during processing at the dispensing level (for example, the NDC is changed during filling due to insufficient inventory)?

Should it be tracked, via the system or on paper, that the daily audit reports are being reviewed?

§ 1311.175 Pharmacy responsibilities

Same question as above about DEA validation. There may be cases where the system's DEA registration check fails but through a manual process the prescriber is found to be valid. Are there scenarios that would warrant a manual override of these system stops? What pieces of information would have to be documented in these scenarios?

§ 1311.150, § 1311.170 SysTrust, WebTrust, or SAS 70 audit

These audits would be of considerable cost for software vendors and healthcare organizations. Since some vendors do not manage the physical security of the system or hardware, the healthcare organization itself may need to be audited. That would mean hundreds of organizations would be required to perform this audit at a considerable cost to the organizations affected and to the market as a whole. Systems are installed, configured, upgraded, and maintained at the healthcare organization's discretion. Such financial burden will be a major hurdle for many organizations in the utilization of e-prescribing for controlled drugs.

These audits are intended for e-commerce web sites. A healthcare information system is considerably more complex than an e-commerce website, as an EMR may provide thousands of features/functions. What would be the subject of such an audit? These audits are done by individual CPA firms. Will such firms be qualified to audit such complex systems in a consistent manner?

With the overall complexity and the number of organizations that would be required to obtain the audits, has the DEA considered the impact of such a requirement if organizations are not able to get an audit performed due to overall demand?

§ 1311.145, § 1311.155, § 1311.170 Report security incidents

What methods will the DEA provide for reporting security incidents? What data items will be required to be reported?

Overall Implementation Concerns

With numerous requirements being placed on the practitioner, practitioner's service provider, intermediaries, and pharmacies, what is the DEA's recommendation for how to best implement safe guards so that the practitioner's e-prescribing system can ascertain that every downstream system is enabled for the e-prescribing of controlled substances?

Without sufficient feedback to the provider of the capabilities of the downstream systems, it will lead to additional practitioner work and additional prescription call-ins to pharmacies.

If the downstream system is not enabled, it would need to deny the electronic prescription and send an error message back to the practitioner. What are the current capabilities of all parties to do this without

code changes? Are we going to run into a situation where practitioners are enabled quicker than the downstream systems to implement checks to reject controlled substances?

When the practitioner receives the error notification, he is left with three options to get the script to the pharmacy, since the proposed regulations do not allow printing the prescription after electronic transmission or changing to fax during transmission.

1. Call-in the prescription (if allowed for the specific drug)
2. Handwrite the prescription
    - If patient is still present hand to the patient.
    - If patient is not present, fax the signed prescription to the pharmacy manually.
3. Cancel the original prescription in the e-prescribing system and have a computer-generated printout produced for signing and faxing.

All three options increase the chances of producing incorrect prescription fills as the provider or the provider's agent will need to reproduce the script either verbally, handwritten, or electronically.

In the case of revocation of ability to accept electronic controlled substances by either the intermediary or by a pharmacy system, what is the proposed notification mechanism to ensure that call-ins and handwriting of scripts can be mitigated? Otherwise the electronic solution could potentially lead to increased patient safety risks.

For some drug schedules, faxing or calling in the order is not allowed. For these drugs, if e-prescribing fails (system error, downstream system can no longer accept the scheduled drug prescription, etc) there is a significant chance the patient has left the office. How will the regulations avoid burdening patients with the time and cost of retrieving a paper prescription to replace the intended electronic prescription? In some cases, patients may neither have the means to return to the office nor know they need to do so until they reach the pharmacy.

Thank you for the opportunity to comment on these proposed regulations and if we may be of any additional assistance, please do not hesitate to contact Peter DeVault, Director of Integration and Interoperability, Sarah Glamm, Research & Development or Jon Millin, Technical Services at 608-271-9000.

Sincerely,

Peter DeVault
Director of Integration and Interoperability
Epic Systems Corporation